UCRL-JC-123053
Preprint

Conducting Secure Financial EDI over the Internet

John Rhodes
Electronic Commerce Projects Leader
Technology Information Systems Program
Lawrence Livermore National Laboratory
Livermore, CA 94550
(510) 422-6550
jrhodes@tis.llnl.gov

This paper was published in the
Jan / Feb 1996 Issue of E-Comm Magazine

1/22/96

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint is made available with the understanding that it will not be cited or reproduced without the permission of the author.

DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-ENG-48.

Conducting Secure Financial EDI over the Internet

Author Bio: John Rhodes is the Electronic Commerce projects leader in the Technology Information Systems Program at Lawrence Livermore National Laboratory where he is currently working on ways to apply Electronic Commerce technologies to increase the effectiveness of business functions.

Abstract: If a pilot program in secure payments currently underway between Lawrence Livermore National Laboratory and Bank of America proves successful, a general methodology will be established which will make it possible for businesses to pay their bills using secure e-mail over the Internet.

Article: As access to the Internet has grown, its use by commercial businesses has increased for many functions such as access to on-line catalogs, information retrieval or exchanging email. However, use of the Internet for conducting financial transactions between enterprises has not grown as quickly. Electronic Data Interchange (EDI) has been the principal fashion by which financial information has been exchanged between enterprises, but for the most part, EDI has not been routinely conducted over the Internet. A key element that has caused hesitancy by businesses to use the Internet for EDI financial transactions has been the possibility of interception or corruption of vital financial data while enroute.

Lawrence Livermore National Laboratory (LLNL) and Bank of America worked independently to create both ends of a system that sends and receives electronic mail (e-mail) -based secure payments over the Internet in a fully automated fashion. The resulting system is based on current EDI as well as Internet standards, and is general purpose enough that it has wide applicability to businesses wishing to do the same thing. The system is also consistent with LLNL's approach to Electronic Commerce on the Internet which involves placing standard EDI transactions into standard e-mail envelopes and sending this e-mail over the Internet using automated processes to interface with existing business systems.

While there are commercially available products for securing and transporting EDI transactions on open networks such as the Internet, these solutions have generally involved using the same proprietary software by both trading partners and require some degree of manual involvement to conduct the process.

Experience

Lawrence Livermore National Laboratory has had significant experience in automating EDI processes and using e-mail to transport and deliver EDI transactions over the Internet. In 1992, LLNL, working in close coordination with Wright-Patterson Air Force Base (WPAFB), designed and fielded the successful Government Acquisition Through Electronic Commerce (GATEC) commodity procurement system.

The GATEC system is an e-mail based system, adheres to commercial X12 EDI standards, communicates between WPAFB and LLNL over the Internet, and uses a VAN Hub operated by LLNL that serves as a gateway to commercial Value-Added Networks (VANs). The VAN Hub e-mails public Requests For Quote (RFQs) to these VANs who in turn make them available to their customers. All inbound vendor Quotes are e-mailed from each VAN to the Hub, which e-mails them to WPAFB for review and consideration. The resulting Purchase Order is then e-mailed from WPAFB to the LLNL Hub across the Internet where it is then passed to the VAN with the winning vendor.

The GATEC system is a 7x24 system and (depending on the e-mail load on the Internet) it is possible for vendors to be able to review an RFQ or Purchase Order within 5-10 minutes of when it is issued. Similarly, a quote submitted by a vendor can be available for evaluation within minutes, as the basic transport mechanism for all transactions is e-mail, not batch processing. Even vendor registration is done electronically via e-mail, with a vendor e-mailing a Vendor Registration transaction from their VAN to the LLNL Hub, where it is automatically processed and an acknowledgment issued back to the vendor - again via e-mail!

In its three years of existence, WPAFB's GATEC system has released more than 90,000 RFQs, processed more than 700,000 Quotes from the current field of 4,300 electronically-registered vendors and has issued more than 64,000 electronic Purchase Orders. It is estimated that the use of this system has saved the Air Force more than $4M in reduced cost of goods purchased (over 10% of the total issued procurements) due to the increased competition made possible through the broad dissemination of Air Force buying requirements to a wide number of vendors and the public release of the Award Notice after an award has been issued.

Process Characteristics

The process of making payments via e-mail over the Internet is really no different in principle than just sending e-mail with an enclosure from one individual to another. The elements that make this system notable are that:

- the body of the e-mail contains the text of the X12 EDI transaction known as a Payment Order (820);
- all transactions between LLNL and Bank of America are encrypted and signed;
- both the sending process and the receiving process are completely automated processes which interface to existing legacy systems in a non-intrusive manner.

Transaction Security

LLNL and Bank of America elected to use all three elements of transaction security in this system; authentication, non-repudiation and privacy. Authentication ensures that the transaction could only have been generated by a specific known source. Non-repudiation ensures that the message has not been modified while enroute. Privacy ensures that the transaction can only be read by the intended receiver. Every transaction in e-mail that is exchanged between the two systems is subject to all three elements of security. Even simple functional acknowledgments are signed and encrypted.

The software that was selected to perform this task was the Trusted Information System's Privacy Enhanced Mail, known commonly as TIS/PEM. This package uses the patented RSA dual key cryptography algorithms for transaction security in conjunction with the standard Multipurpose Internet Mail Extension (MIME). The use of PEM ensures the authenticity of messages through digital signatures and secures the privacy of messages through data encryption. A key advantage in the use of e-mail for exchanging secure information rather than the batch transfer of encrypted files is that by securing only the message body, (thus leaving the e-mail routing information in clear text) the secure email can be successfully routed over public networks just like ordinary e-mail.

In contrast to the Digital Encryption Standard (DES) where the same key is used to both encrypt and decrypt a message, the RSA algorithms use key pairs, called public-private keys. Text encrypted with an intended receiver's public key can only be decrypted with the corresponding private key. Only the private key holder knows the contents of his private key.

Generating the Secure E-Mail

The transaction security process starts by computing the unique Message Integrity Check (MIC) of LLNL's EDI payment information. The message body and the MIC are now pairwise unique to one another. The MIC is then encrypted with LLNL's private key and the encrypted MIC is then attached to the e-mail as a MIME message part. The MIC is the signature for the transaction as only LLNL (who is the unique holder of the private key) could have generated the encrypted MIC from a given message. The computation of the MIC and attachment as part of the message acts as the non-repudiation, as the message body could not have been altered and still generate the same MIC. The message is now 'signed'.

The next step is to ensure privacy. Since the RSA algorithms are relatively compute-intensive and the DES algorithm is very fast, the process randomly generates a DES key and encrypts the X12 EDI payment information with this key. The DES key is used only once.

The DES key is then encrypted with Bank of America's public key and included with the message. LLNL now knows that only Bank of America's private key can decrypt the DES key and then by using this DES key can decrypt and read the message body. The message is now 'secure'.

Reading the Secure E-Mail

Bank of America uses the public key of LLNL to decrypt and read the MIC. Bank of America then uses their private key to decrypt and read the DES key, which is then used to decrypt and read the transaction message body. The MIC for this message body is then computed and compared to the one included with the message. They will match only if the body has not been modified (non-repudiation) and if the original MIC was encrypted with LLNL's private key (authentication).

How the Payments Process Works

The information flow for this system is shown in the accompanying Figure 1.

Each day, the daily payments file is automatically downloaded from the Accounts Payable system to LLNL's Secure EDI Server. That system translates that file into the X12 Payment Order (820) format, signs it, encrypts it and e-mails it to Bank of America's Secure e-mail server. This system authenticates it, decrypts it and transfers the EDI file to their standard EDI system. That system performs the translation from the X12 EDI format to their internal format. Functional Acknowledgment (997) and Application Advice (824) transactions are created and sent to their e-mail server where they are signed, encrypted and e-mailed to LLNL. The LLNL system authenticates them, decrypts them and translates

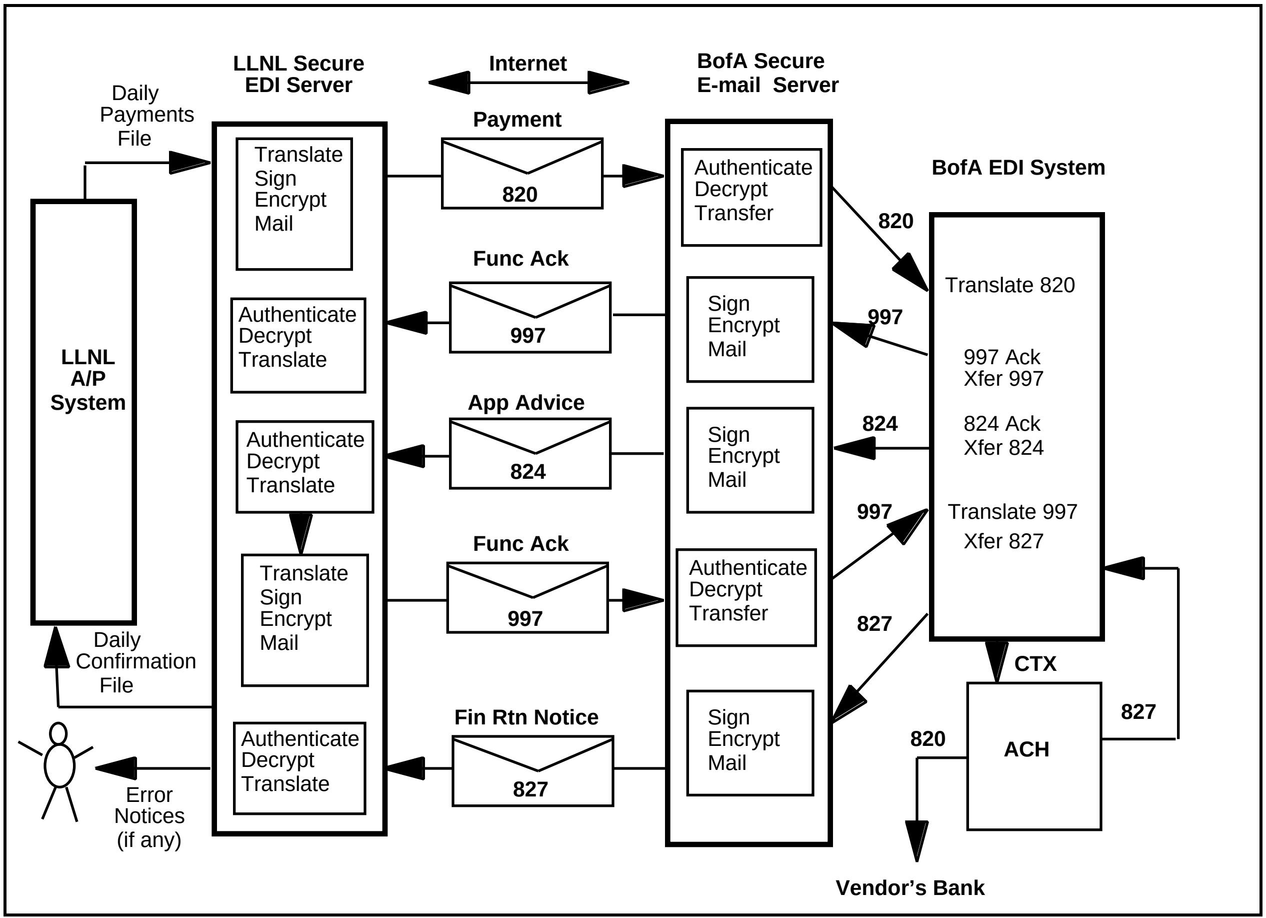

Figure 1

them into an internal format for automated analysis. Any errors reported by the 997 or the 824 are automatically annotated and routed via e-mail to a LLNL payments analyst for resolution. If the 824 indicates that all payments were properly applied, then LLNL creates a 997, signs it, encrypts it and e-mails it to Bank of America, thus completing the cycle.

This entire automated process, from the original download of the Daily Payments file to the final mailing of the 997 from LLNL to Bank of America, occurs in under ten minutes.

After the payments have been loaded into Bank of America's EDI system, they are subsequently processed through the issuance of a large volume of Corporate Trade Exchange (CTX) 820 transactions with the Automated Clearing House (ACH). If provided the information, in addition to transferring funds, the ACH can provide the full textual contents of the 820, which includes complete remittance information, to the vendor's bank for transmission to the EDI-capable vendor. By using the full 820, instead of just an Electronic Funds Transfer (EFT), the vendor can have access to all of the information relevant to that payment, such as the associated invoice number or the Purchase Order number.

A failure by the ACH to perform a transaction as requested results in a Financial Return Notification (827) which is routed in a secure fashion back to LLNL for manual processing.

Process Controls

As part of the design of the system, in order to limit exposure to spurious email transmissions that might flow to either system from other sources on the Internet as well as to ensure that non-receipt due to possible Internet outages was considered, it was decided to issue all outbound data transactions from LLNL to Bank of America within a predesignated time window. This window was set wide enough to allow for normal day-to-day processing variations but narrow enough that Bank of America can initiate alternative procedures during the regular workday that can be used if the transactions are not received within that time window.

Once Bank of America has processed the EDI information, a functional acknowledgment is issued which must be received by LLNL within a certain time frame.

If there are no payments to be issued in a given day, a 'null' transaction is issued within the regular time window that exercises Bank of America's system and ensures that Internet communications are operational. This 'null' transaction generates acknowledgments just like a real transaction and thus also exercises LLNL's system also.

Because this system operates in a completely automated fashion, it was decided to have Bank of America's EDI system default to ‘no-pay’ status on receipt of any transactional errors. Because payments are made sufficiently ahead of time, a no-pay condition can be resolved by the LLNL financial analysts in a thoughtful manner, without being placed under the duress that having to get a payment issued the same day requires.

Results to Date

Thus far, the system has worked well with only minor fine-tuning required. Typical round-trip transit times for Internet e-mail have been under ten minutes, which includes the EDI processing times at both ends. Random tests of the system security - some intentional and some not - have resulted in the appropriate system responses.

Future

During the pilot evaluation period which lasts through January 1996, LLNL is making electronic payments of $10k to $50k per day to a small number of selected vendors. If the pilot is successful, LLNL hopes to expand to include all of its thousand or more vendors with anticipated total payment volume of over $1M per day.

Acronyms

CTX - Corporate Trade Exchange
EC - Electronic Commerce
EDI - Electronic Data Interchange
EFT - Electronic Funds Transfer
GATEC - Government Acquisition Through Electronic Commerce
LLNL - Lawrence Livermore National Laboratory
MIC - Message Integrity Check
MIME - Multipurpose Internet Mail Extension
PEM - Privacy Enhanced Mail
RFQ - Request for Quote
TIS - Trusted Information System
VAN - Value-Added Network
WPAFB - Wright-Patterson Air Force Base